Indian Health Service
Division of Information Security

Standard Operating Procedure for Incident and Event Reporting

SOP 05-02

December 2004

FOR OFFICIAL USE ONLY
This information is intended for IHS use only. Disclosure is not expected to cause serious harm to IHS, and access is provided freely to all internal users via the organization's Intranet.

DOCUMENT INFORMATION

REVISIONS/RESCISSIONS
None

EXCEPTIONS TO PROCEDURE
None

AUTOMATIC RESCISSION DATE
This procedure will be rescinded three years from the date of approval.

REVIEW
This procedure will be reviewed annually to maintain its currency and will expire in three years from the date of its approval.

TABLE OF CONTENTS

1.0 RECORD OF CHANGES 1

2.0 INTRODUCTION 2

2.1 Purpose and Scope 2
2.2 Document Organization 2

3.0 INCIDENT REPORTING CAPABILITY OVERVIEW 3

3.1 Background 3
3.2 Incident Reporting Structure 3
3.3 SOCC Functions 5
3.4 Incident Reporting Definitions 6
3.5 Roles and Responsibilities 8
3.5.1 IHS CIO 8
3.5.2 IHS Chief Information Security Officer (CISO) 8
3.5.3 Area ISSO 10
3.5.4 Service Unit ISSO 10
3.5.5 IHS System Administrators, Network Administrators, Security Officers and Users 11

4.0 INCIDENT REPORTING REQUIREMENTS 12

4.1 HHS SOCC Reporting Requirements 12
4.1.1 Individual Incident Reporting 12
4.1.2 Monthly Summary Reports 13
4.1.3 Reporting to Internal and External Entities 14
4.2 IHS Security Team Reporting Requirements 14
4.2.1 Individual Incident Reporting 14
4.2.2 Monthly Summary Reports 16
4.2.3 Reporting to External Entities 17
4.3 Third Party Information Security Service Providers Reporting Requirements 17

5.0 APPENDIX A: MAPPING OF INCIDENT CATEGORIES 18

6.0 APPENDIX B: ACRONYMS 19

7.0 APPENDIX C: INCIDENT REPORTING FORM 20

8.0 APPENDIX D: MONTHLY SECURITY EVENTS REPORT SPREADSHEET 23

9.0 GLOSSARY 24

1.0 Record of Changes

Change No.	Date	Subject	Page No.
1	10/28/2004	Initial Draft	NA
2	11/15/2004	Second Draft	
3	12/1/2004	3rd Draft	
4	12/02/04	4th Draft	
5	12/22/04	Final Draft	

2.0 Introduction

This section provides the purpose, scope, and organization of this document.

2.1 Purpose and Scope

This SOP provides incident reporting procedures for IHS' federally-run facilities and for IHS' partners' facilities as described below. The term facilities includes Area Offices (AOs), Service Units (SUs), urban facilities, hospitals, clinics and other associated facilities.

Facilities of tribal or tribally-run organizations that leave their IT shares shall follow this SOP in accordance with their contracts or compacts.

It is recommended that facilities of tribal or tribally-run organizations that do not leave their IT shares follow this SOP.

Contractors' facilities shall follow this SOP in accordance with their interconnection agreements with IHS.

For the purposes of this document, the use of IHS is intended to include any of the above facilities

The incident reporting procedures apply to all IHS facilities and are in accordance with Health and Human Services (HHS) reporting requirements and directives.

2.2 Document Organization

The remainder of the document is structured as follows:

- Section 3.0 outlines the incident reporting capability function within HHS and establishes the incident response reporting structure within IHS.
- Section 1.0 outlines the incident reporting requirements for HHS and IHS' incident reporting capability.

3.0 Incident Reporting Capability Overview

This section outlines the incident reporting capability function within HHS and IHS; establishes the incident response reporting structure; provides an overview of applicable definitions, roles, and responsibilities; and describes the HHS Secure One Communications Center (SOCC) functions and process flow.

3.1 Background

An incident response reporting capability serves as a mechanism to receive and/or disseminate incident information and provides a consistent capability to report incidents.

The IHS and HHS incident reporting capability functions in accordance with the following Federal policies and regulations: Office of Management and Budget Circular A-130, Appendix III, Security of Federal Automated Information Resources; the President's Management Agenda fiscal year 2004 that established the Management Plan Agenda (MPA); Health Insurance Portability and Accountability Act (HIPAA) 1996 and the Federal Information Security Management Act (FISMA).

The incident response reporting capability also provides immediate tangible benefits and results for other Operating Divisions (OPDIV) participants, HHS Chief Information Officer (CIO), and the United States Computer Emergency Readiness Team (US-CERT). These benefits include the following:

- vulnerability analysis, enhanced alerts and warnings, and enhanced measures of performance and effectiveness for OPDIV incident reporting;
- increased understanding throughout the IHS of its information security posture and environment through consistent, well-communicated procedures and timely and accurate reporting from all levels within the agency;
- integration of the HHS SOCC with other internal IHS efforts to eliminate redundant efforts, capitalize on existing intellectual capital, and enhance the common operating picture of the IHS environment; and
- clear and consistent internal and external reporting mechanisms for information security incidents.

3.2 Incident Reporting Structure

Secure One HHS established a department security operations center (SOCC) which is responsible for collaboration among all OPDIVs, third party information security service providers, and US-CERT. Each OPDIV shall maintain an incident response capability that

reports directly to the HHS SOCC. The incident reporting process that IHS shall use is as follows:

1. When potential incident activity is detected at:

    a. *Service Unit* (or associated facility below the Area level). The discoverer notifies the SU Information Systems Security Officer (ISSO) immediately. Or in the absence of an ISSO at SU, the respective Area ISSO will be notified immediately.

    b. *Area.* The discoverer notifies the Area's ISSO immediately. Or in the absence of the Area ISSO, the IHS Information Security Team (IST) is notified immediately.

    c. *Headquarters (HQ)* (or other IHS facilities not covered by 1a. or 1b.). The discoverer notifies the facility ISSO (if assigned) immediately. Or in absence of a facility ISSO, the respective Area ISSO is notified immediately. Or in the absence of the Area ISSO, the IHS IST is notified immediately.

2. Upon determination that the detected activity is an actual incident;

    a. *Service Unit* (or associated facility below the Area level). The SU ISSO notifies the Area ISSO within one hour of the determination;

    b. *Area.* The Area ISSO notifies the IST within one hour of the determination.

    c. *HQ* (or other IHS facility not covered by 2a. or 2b.). The HQ or other facility ISSO notifies the IST within one hour of the determination.

3. The Area ISSO notifies the IST within one and one half hours of the initial determination.

4. The IST notifies the SOCC within two hours of the initial determination.

5. The SOCC creates a log entry and determines the appropriate approach to take to report the incident. The three options are:

    - *Internal:* Notify the other OPDIVs and the OIG Computer Crimes Unit (CCU) of the incident;

    - *External:* Contact US-CERT or the appropriate entity; or

    - *Both:* Notify the other OPDIVs, OIG CCU, and US-CERT of the incident.

6. At the end of the month, the SOCC consolidates all the log entries and provides the OPDIVs with a monthly summary report.

7. The IHS Chief Information Security Officer, CISO provides the SOCC monthly summary report to Area ISSOs

8. The Area ISSO provides the SOCC monthly summary report to their respective SU ISSOs.

Section 1.0 provides a more detailed explanation of the incident reporting procedure and requirements. Figure 3-1 shows the IHS incident reporting structure.

The IST serves as the coordination center and central point of contact (POC) for all IHS organizations for incidents within the agency. The SOCC serves as the coordination center and the central POC for incidents for HHS. The SOCC facilitates incident reporting to the OIG CCU and to external reporting entities such as US-CERT. Collaborative relationships between the IST, the SOCC, and other stakeholders such as US-CERT, the OIG CCU, and third party information security service providers facilitate the incident response process.

3.3 SOCC Functions

The SOCC provides incident management functions, such as:

- *Incident Response Collaboration*. The SOCC collaborates with the OIG CCU and third party information security service providers to act as one virtual SOCC during an incident. The SOCC also provides a Department-wide standard definition of an event and an incident.

- *Incident Alert Notifications*. If IHS or third party information security service providers notify the SOCC of an incident, the SOCC sanitizes incident information and alerts other OPDIVs of the potential threat.

- *Incident Reports*. The SOCC facilitates incident reporting to external entities, maintains a database of reported incidents, and compiles and distributes sanitized reports to OPDIVs on a monthly basis.

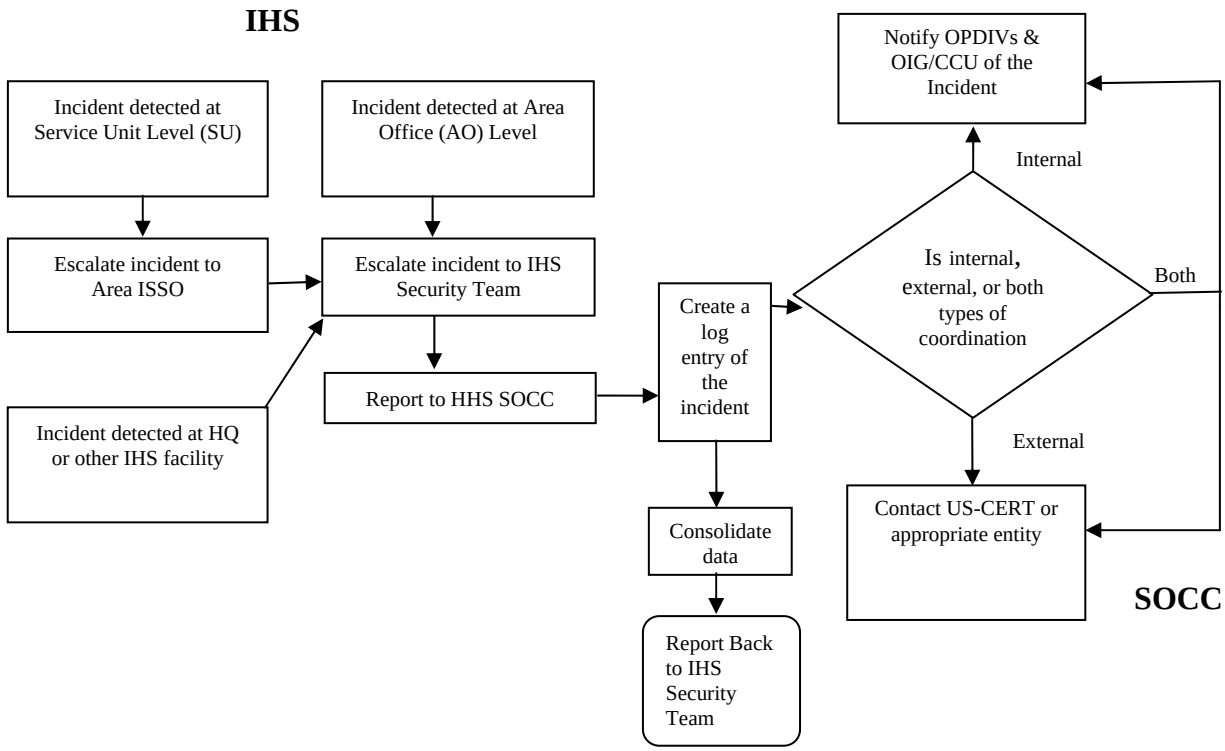

Figure 3-1: IHS Incident Reporting Structure

3.4 Incident Reporting Definitions

IHS shall use the following event and incident definitions:

- *Event*: An observable occurrence in a network or system.
- *Incident*: The violation, or an imminent threat of a violation, of an explicit or implied security policy, acceptable use policies, or standard security practices in a computing or telecommunications system or network. While certain adverse events, (e.g., floods, fires, electrical outages, and excessive heat) can cause system crashes, they are not considered computer-security incidents.[i]

IHS shall use the following categories when reporting events and incidents to the SOCC:

- *Malicious Code*: A virus, worm, Trojan horse, or other code-based entity that is either successful or unsuccessful in infecting a host. This category applies to *incidents* and *events*.

[i] *Definition adapted from the HHS Incident Response Planning Guide (October 20, 2003) and updated to comply with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 incident definition (January 2004)*

- *Probes and Reconnaissance Scans*. Probes and reconnaissance scans involve searching the network for critical services or security weaknesses. This category applies to *incidents* and *events*.

- *Denial of Service (DoS)*. A successful or unsuccessful attack (including Distributed Denial of Service Attacks) impairs the authorized use of networks, systems, or applications by exhausting resources, to include Distributed DoS attacks. This category applies only to an *incident*.

- *Unauthorized Access*. A person gains logical or physical unauthorized access to a network, system, application, data, or other resource. This access may include root compromises, unauthorized data alterations or data viewing, Web site defacements, loss/theft of equipment, unauthorized use of passwords, unauthorized access to "shares", unauthorized access to any RPMS application or data; and use of packet sniffers. This category applies only to an *incident*.

- *Inappropriate Usage*. A person violates acceptable computing use policies, such as sending spam, email threats, or making illegal copies of software. This category applies only to an *event*.

Figure 3-2 shows the category differentiation and reporting time frames when reporting incidents or events. HHS requires IHS to report an incident to the SOCC within two hours of determination of an incident. This means Areas and Service Units shall report an incident to the IST within one and one half hours and HQ and other IHS facilities shall report an incident to the IST within one hour of the determination of an incident to allow sufficient time for the SOCC notification within the specified parameters. Events are reported to the IST on a monthly basis as a security events report. The Area security events reports are combined into one IHS report and submitted to the SOCC.

		Incident and Event Categories					
Incident or Event	**Reporting Timeline**	**Malicious Code**	**Probes and Reconnaissance Scans**	**Denial of Service**	**Unauthorized Access**	**Inappropriate Usage**	**Other**
Incident	To IHS IST within 1.5 hours of detection ******* To HHS SOCC within 2 hours of detection	Malicious Code Infection	Probes and reconnaissance scans pose a serious threat	Attack causes loss of service	Unauthorized access		Cannot be reported in another category
Event	IHS - On a monthly basis, by the 2nd of the month ******* To HHS SOCC by the 5th of the month	Malicious code infection prevented	Probes and reconnaissance scans detected			Inappropriate usage	Cannot be reported in another category

Figure 3-2: Reporting Timelines for Incident and Event Categories and Priorities

3.5 Roles and Responsibilities

The roles and associated responsibilities for the incident reporting functionality within IHS are described in the following sections:

3.5.1 IHS CIO

The roles and responsibilities of the IHS CIO will be to:

- Establish an IHS incident reporting capability to serve as the first tier of incident reporting;
- Develop and maintain IHS incident reporting policy and procedures; and
- Enforce processes and procedures developed by IHS, HHS, and the SOCC.

3.5.2 IHS Chief Information Security Officer (CISO)

The roles and responsibilities of the IHS CISO will be to:

- Establish an IST that coordinates an IHS-wide incident reporting capability that coordinates with the SOCC as required by HHS policy and directives;
- Establish partnering relationships with all IHS entities;
- Establish partnering relationships with Federal incident reporting capabilities;
- Establish partnering relationships with the SOCC;
- Ensure all AOs, SUs, HQ, and other IHS facilities maintain a separate incident reporting capability that serves as the first tier that will collect information regarding incidents before they are reported to the IST and the SOCC;
- Serve as the primary clearinghouse and collection point for incident information involving IHS systems for the agency;
- Collaborate with the SOCC, OIG CCU, and third party information security service providers;
- Establish a means of collecting incident information from the IHS and other facilities on a per-incident basis, and collecting event information on a monthly basis;
- Aggregate and sanitize monthly reports and forward one consolidated report to the SOCC;
- Coordinate incident and event reporting within IHS and to the HHS CISO, SOCC, third party information security service providers, OIG CCU, and US-CERT;
- Disseminate monthly SOCC incident summary reports to Area ISSOs;
- Serve as the first tier for incident reporting to the SOCC at the IHS level;
- Serve as the second or third tier for incident reporting at the IHS Area, SU, HQ, and other IHS facilities levels;
- Report incidents to the SOCC within 2 hours of incident identification;
- Provide monthly events summary reports to the SOCC by the fifth calendar day (or the following work day) of each month for events that occurred the previous month;
- Write lessons learned and follow-up reports for incidents;
- Disseminate monthly SOCC incident summary reports to Area ISSOs; and

- Establish and implement tools and processes supporting IHS policies and procedures to ensure timely reporting of security incidents.

3.5.3 Area ISSO

The roles and responsibilities of the Area ISSO will be to:

- Serve as the Area SUs second tier for incident reporting to the IST;
- Collaborate with the SU ISSO, IST, and local management;
- Serve as the first tier for incident reporting at the Area level for reporting to the IST;
- Coordinate incident and event reporting within the Area and to the IST;
- Report first tier incidents to the IST within one hour and second tier incidents within one and one half hours of incident identification;
- Provide monthly summary reports of events to the IST by the 2nd calendar day (or the following work day) of each month for events that occurred the previous month;
- Write lessons learned and follow-up reports for incidents and provides copies of lessons to IST; and
- Establish and implement tools and processes supporting IHS policies and procedures to ensure timely reporting of security incidents.

3.5.4 Service Unit ISSO

The roles and responsibilities of the Service Unit ISSO will be to:

- Serve as the first tier of incident reporting for the SU to the Area ISSO;
- Collaborate with the Area Office ISSO, IST, and local management;
- Coordinate SU incident and event reporting to the Area ISSO;
- Report incidents to the Area ISSO within one hour of incident identification;
- Provide monthly events summary reports to the Area ISSO by the 1st calendar day (or the following work day) of each month for events that occurred the previous month;

- Write lessons learned and follow-up reports for incidents and provide copies of lessons to Area ISSO; and

- Establish and implement tools and processes supporting IHS policies and procedures to ensure timely reporting of security incidents.

3.5.5 IHS System Administrators, Network Administrators, Security Officers and Users

System administrators, network administrators, site managers, Information Systems Coordinators, security officers, and all other users of IHS-provided computers, telecommunications systems, or network resources must report any known or suspicious incidents immediately. Reporting must comply with IHS security incident policy and procedures.

4.0 Incident Reporting Requirements

This section outlines incident reporting and associated requirements for IHS and the SOCC.

4.1 HHS SOCC Reporting Requirements

The SOCC serves as the interface to external organizations for HHS OPDIVs. All IHS information security events and incidents are reported to the IHS CISO who acts as the central repository for incident and event reporting. The IHS CISO reports all incident and event information for IHS to the SOCC.

4.1.1 Individual Incident Reporting

A user or other party notifies the SU ISSO of a potential incident. Upon identification of an actual incident, the SU ISSO notifies the Area ISSO of the incident within one half hour of identification of the incident. The Area ISSO notifies the IST of the incident within one hour after initial identification of the incident. The IST then notifies the SOCC within two hours of the initial identification of an incident. Likewise, if the incident is detected at the Area level, the Area ISSO notifies the IST within one hour and the IST notifies the SOCC within two hours of the initial identification of an incident. Events are reported to the IST in a monthly summary report. (See Section 3.4 for definition of an *incident* or an *event*.) Incidents are reported as they occur as outlined in this document.

The following are steps that shall be taken to report an incident:

If an Area, SU, or other entity within IHS detects an incident not detected by a third party information security service provider:

- The SU provides as much detail as possible to the Area ISSO who in turn relays the information to the IST. The information is reported either by telephone or by forwarding an Incident Reporting Survey (Appendix C: Incident Reporting Form).
- The IST notifies appropriate IHS management and reports the incident to the SOCC.
- The SOCC alerts the HHS CISO, third party information security service providers, and the OIG CCU as appropriate.
- Once appropriate parties are notified, the SOCC alerts other HHS OPDIVs as applicable.

If an Area, SU, or other entity within IHS has a question about a suspicious activity:

- The facility provides information about the suspicious activity to the Area ISSO who in turn relays the information to the IST either by telephone or by forwarding an Incident Reporting Survey (Appendix C: Incident Reporting Form) (See Section 4.2.1).

- The IST forwards the information to the SOCC either by telephone or by forwarding the Incident Response Survey (See Section 3.2 or Appendix C).

- The SOCC coordinates with appropriate third party information security service providers to possibly identify suspicious activity.

- The SOCC contacts other OPDIV CISOs to determine whether suspicious activity has a larger impact across the Department.

If a third party information security service provider identifies a potential incident at the Department level:

- The provider forwards as much information as possible to the SOCC.

- The SOCC evaluates the potential incident and consults with the HHS CISO to determine the applicability of the threat.

- If necessary, the SOCC alerts the OPDIVs to the potential threat.

If a third party information security service provider identifies a potential incident within IHS:

- The provider forwards as much information as possible to the IST and the SOCC.

- The IST evaluates the potential incident and coordinates with the SOCC.

- As necessary the IST forwards the information to an Area, SU, or other facility ISSO for response and subsequent reporting.

- If necessary, the SOCC contacts all other OPDIVs of a potential incident within HHS.

- The SOCC reports the incident to US-CERT, if required.

4.1.2 Monthly Summary Reports

Each IHS Area is responsible for aggregating the monthly event summary reports received from their facilities into one Area level sanitized monthly event summary report. The IHS CISO is responsible for aggregating the monthly Area event summary reports into one IHS monthly event summary report. The Area's summary reports are due to IHS CISO by the end of the second calendar day of each month (or the following work day) for events that occurred during the previous month. The IHS monthly event summary report is due to the SOCC by the fifth calendar day of each month (or the following work day). Only events, not incidents, are included in this report.

The SOCC collects additional information to support its Department-wide correlation of threats, vulnerabilities, and incidents.

4.1.3 Reporting to Internal and External Entities

The SOCC is responsible for reporting incidents to internal and external entities, including OIG CCU, third party information security services providers, and US-CERT. The SOCC is also responsible for disseminating sanitized incident and event information to the OPDIVs.

4.1.3.1 Reporting to US-CERT

Upon notification of an incident, the SOCC reports the incident to US-CERT. Information requests to IHS from US-CERT are submitted through the SOCC to ensure consistent reporting across the Department.

4.1.3.2 Reporting to OIG CCU

A collaboration agreement is established between the SOCC and the OIG CCU. The SOCC coordinates escalation of reporting to the OIG CCU for all validated criminal security incidents. Coordination with law enforcement shall be conducted primarily by, or in conjunction with, the OIG CCU.

4.2 IHS Security Team Reporting Requirements

The IST serves as the first tier of incident reporting function at the Agency level, HQ, and other facilities, as the second tier for the Areas Offices, and third tier for SUs and Urban facilities.

4.2.1 Individual Incident Reporting

Upon identification of an incident, the IHS CISO is required to contact the SOCC within two hours of incident identification with as much information as possible about the incident (*e.g.*, what happened, what is the initial damage). The IHS CISO is required to update the SOCC as new information is discovered about the incident. (See Section 3.4 for a definition of an *incident*.)

Incidents shall be categorized when reported by the cause of the incident, not the end result. The following are the incident categories:

- *Malicious Code Infections*. Successful virus or worm infection on a device (report number of devices infected per occurrence). If the virus was prevented, it would be reported as an *event*.

- *Probes and Reconnaissance Scans*. Poses a serious threat to a critical system. If the probes or scans were only detected, but did not pose a serious threat to a critical system, it would be reported as an *event*.

- *DoS*. Loss of service from an attack.

- *Unauthorized Access*. Root compromise, unauthorized access, or alteration of data, unauthorized access to "shares", applications including RPMS, and unauthorized access or use of passwords, web site defacement,.

- *Other*. Cannot be reported in an above category but is a serious threat to the confidentiality, integrity, or availability of critical information. This category may include fraud, theft of property or data, IP spoofing, unauthorized physical access, etc.

When reporting an incident, the IHS CISO shall provide all of the following information that is available by using the Incident Reporting Survey (Appendix C: Incident Reporting Form) or by telephone:

- POC information (name, email address, title, telephone number, agency);
- Support action requested and the timeframe;
- Entities that the SOCC and US-CERT can share incident data with;
- Approximate start time of the incident and the current status;
- Information on the attacking computer(s) and victim computer(s), such as
    - Internet protocol address,
    - Address range (netmask),
    - Host name or domain;
- Victim/targeted operating system;
- Ports targeted in the attack;
- Primary purpose of the targets/victims involved; and
- Number of hosts affected.

When reporting an incident, the Area or SU ISSO shall provide all of the following information that is available by using the Incident Reporting Survey (Appendix C: Incident Reporting Form) or by telephone:

- POC information (name, email address, title, telephone number, agency);
- Support action requested and the timeframe;
- Entities that the SOCC and US-CERT can share incident data with;
- Approximate start time of the incident and the current status;

- Information on the attacking computer(s) and victim computer(s), such as
    - Internet protocol address,
    - Address range (netmask),
    - Host name or domain;
- Victim/targeted operating system;
- Ports targeted in the attack;
- Primary purpose of the targets/victims involved; and
- Number of hosts affected.

4.2.2 Monthly Summary Reports

Service Unit ISSOs must generate and forward to the Area ISSO a monthly events report. The Area ISSO shall generate a consolidated summary Area events monthly report from the SU reports. The IHS Events monthly reports summarize the Area consolidated reports, and may include changes to POC information, improvement suggestions, and other incident response issues of concern to the IHS. The monthly summary report collects the following information:

- Viruses prevented;
- Probes and reconnaissance scans that were determined not to be causing a threat to a critical system;
- Inappropriate usage;
- Probes and reconnaissance scans incidents;
- Malicious code incidents;
- Denial of Service (DoS) incidents;
- Unauthorized access incidents; and
- Additional information as required for the SOCC's Department-wide data correlation efforts.

The IHS monthly Events report is due to the SOCC the fifth calendar day of each month (or the following workday) for events that occurred during the previous month. Since each incident is reported separately to the SOCC, incidents are not included in the monthly summary report. The HHS online tool is used for IHS' monthly report. This tool is not available for Area/SU use but is expected to be in the future. Until the online tool is available, Area and SU ISSOs shall use

the security events report spreadsheet template (See Appendix D: Monthly Security Events Report Spreadsheet) (See Section 3.4 for definition of an *event.*)

Events shall be categorized in the monthly summary report. The following categories shall be used to report events to the SOCC:

- *Malicious Code Prevented*: Viruses prevented and did not cause any harm to any system;
- *Probes and Reconnaissance Scans Detected*: Probes and scans detected and did not pose a serious threat to a critical system;
- *Inappropriate Usage*: Misuse of resources; or
- *Other*: Cannot be reported in an above category and is a threat to the confidentiality, integrity, or availability of non-critical information.

4.2.3 Reporting to External Entities

Incident reporting to US-CERT, the OIG CCU and law enforcement, third party information security service providers, and other external entities is coordinated through the SOCC.

4.3 Third Party Information Security Service Providers Reporting Requirements

Third party information security services such as an intrusion detection monitoring service shall collaborate with the SOCC, OIG CCU, the IHS CISO, and Area, SU, and other ISSOs to ensure threat, incident, and event information is disseminated and reports are generated and forwarded as required.

5.0 Appendix A: Mapping of Incident Categories

HHS categories map to existing HHS monthly reporting and to the HHS Incident Response Guide, US-CERT, and NIST SP 800-61 categories. However, various terms to describe the categories are used by different organizations. Table 5-1 shows this category cross-mapping and what HHS SOCC incident categories are referred to by other organizations.

Table 5-1: Incident Categories

SOCC Incident Categories	Current OPDIV Monthly Reporting	Current HHS Incident Response Guide (2003-G11)	FedCIRC	NIST SP 800-61
Malicious Code	Viruses	Malicious Logic	Priority 1, 2, and 3	Malicious Code
Probes and Reconnaissance Scans	Probes and Scans	Probes and Reconnaissance Scans	Priority 2 and 3	
Denial of Service	DoS	DoS	Priority 1	DoS
Unauthorized Access	System Compromise	Unauthorized Access, Alteration or Theft	Priority 1 and 2	Unauthorized Access
Inappropriate Usage	Other	Unauthorized Use of Service	Priority 4	Inappropriate Usage

The reporting categories and SOCC reporting requirements for an incident and event were derived from the US-CERT Priority Levels presented in Table 5-2:. Priority 1 is the highest priority level; Priority 4 is the lowest priority level.

Table 5-2: Incident Priority Levels

Priority Level	Definition
Priority 1	Possible life-threatening activity; or affects classified or critical systems or information
Priority 2	Incident could become public; provide unauthorized access to network and/or unclassified, non-critical information; affect systems resources; or show active targeting of classified/critical systems
Priority 3	Incident shows active targeting of unclassified, non-critical systems or potential threats to network
Priority 4	Incident shows possible malicious intent or unintentional violation of security policy

6.0 Appendix B: Acronyms

AO	Area Office
CCU	Computer Crimes Unit
CISO	Chief Information Security Officer
DoS	Denial of Service
US-CERT	United States Computer Emergency Readiness Team
HHS	Health and Human Services
IHS	Indian Health Service
IRT	Incident Response Team
ISDM	Information Security Data Manager
ISS	Internet Security Systems
ISSO	Information Systems Security Officer
IST	IHS Security Team
IT	Information Technology
MPA	Management Plan Agenda
MSS	Managed Security Services
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OPDIV	Operating Division
POC	Point of Contact
SOCC	Secure One Communications Center
SOP	Standard Operating Procedures
SP	Special Publication
SU	Service Unit

7.0 Appendix C: Incident Reporting Form

The Incident Reporting Form is to be submitted to IST in accordance with timeframes outlined in this procedure.
(Please use form F05-02)

IHS OPDIV

Incident Reporting Form

	Incident Specific Information
IHS Area/Facility Name:	
ASUFAC:	
Tribal Facility Name:	
Contractor Name:	
Contractor Facility Location:	
INITIAL INFORMATION	
Today's Date	
Current Time	
POC Name	
POC E-mail Address	
POC Title	
POC Phone Number	
OPDIV	

Was this incident identified by ISS MSS?	
If yes, what is the ISS Incident Ticket Number?	
Support Action being requested (i.e., remove computer from network, secure physical area, patch system, etc.)	
Support Action Requested Timeframe	
Who can the SOC and FedCIRC share incident data with?	
What was the approximate start time of the incident?	
What is the current status of the incident (Open/Closed)?	
Is there more than one attacking computer (Yes/No)?	
If yes, how many attacking computers?	
Please list each attacking computer's IP Address (if practical)	
Please list each attacking computer's Address Range (net mask) (if practical)	
Please list each attacking computer's Host Name or Domain (if practical)	

Is there more than one victim computer (Yes/No)?	
If yes, how many victim computers?	
Please list each victim computer's IP Address (if practical)	
Please list each victim computer's Address Range (netmask) (if practical)	
Please list each victim computer's Host Name or Domain (if practical)	
What is the Victim/Targeted software (e.g., OS, application)?	
Which ports were targeted in the attack?	
What was the primary purpose of the target/victims involved in the attack? (ex., workstation (ws) used for data entry, exchange server, ws used for financial	

8.0 Appendix D: Monthly Security Events Report Spreadsheet

The following report is to be submitted monthly in accordance with procedures and timeframes outlined in this document.

(Please use form F05-01)

Monthly Event Summary
IHS Area Name:

Month/Year being reported	Number of Malicious Code Events Prevented	Number of Probes and Scans Detected	Number of Inappropriate Usage Events	Number of "Other" Events	Malicious Code Incident	Probes and Reconnaissance Scan Incidents	Denial of Service Incident	Unauthorized Access Incident	Other Incidents

9.0 Glossary

Term	Definition
Access	Is the ability to do something with a computer resource. For example the ability to read, write, append, create, modify, or delete a file; execute a program; or use an external connection.
Availability	"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542] A loss of *availability* is the disruption of access to or use of information or an information system.
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., SEC 3542] A loss of *confidentiality* is the unauthorized disclosure of information. [FIPS Publication 199, Section 3 Security objectives]
Event	An observable occurrence in a network or system.
Federal Information System	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. [40 U.S.C., SEC 11331]
Incident	The violation, or an imminent threat of a violation, of an explicit or implied security policy, acceptable use policies, or standard security practices in a computing or telecommunications system or network. While certain adverse events, (e.g., floods, fires, electrical outages, and excessive heat) can cause system crashes, they are not considered computer-security incidents.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology. [44 U.S.C., SEC. 3542]
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability. [44 U.S.C., SEC. 3502]
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., SEC. 3502]
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., SEC 3542] A loss of *integrity* is the unauthorized modification or destruction of information. [FIPS Publication 199, Section 3 Security objectives]